ChinaXiv合作期刊

格上的简短可链接环签名 *

王杰昌 [1]，张 平 [2]，李 杰 [1]，常琳林 [1]，段 莹 [3†]

(1. 郑州大学体育学院体育大数据中心，郑州 450000; 2. 河南科技大学数学与统计学院，河南 洛阳 471023; 3. 郑州航空工业管理学院智能工程学院，郑州 450003)

摘 要：可链接环签名可防止区块链中的双花攻击，基于格的签名可抵抗量子攻击，但已有格基可链接环签名的大小随环成员的增多而增大。针对该问题，提出了一种格上的简短可链接环签名方案。该方案用队列实现了向量数制的特殊转换，利用格上的累加器对环成员的公钥进行累加，使得签名大小不会随环成员的增多而增大；利用拒绝采样定理，构造出格上的知识证明签名，在防止签名私钥泄露的同时，提高了计算效率。在随机预言机模型下，证明了方案具有不可伪造性、匿名性、可链接性。性能分析与实验评估表明，本方案节省了时间开销和存储开销，且随着环成员的增多签名大小固定不变。

关键词：格；知识证明签名；累加器；简短可链接环签名

中图分类号：TP309.2 doi: 10.19734/j.issn.1001-3695.2022.02.0057

Lattice-based short linkable ring signatures

Wang Jiechang[1], Zhang Ping[2], Li Jie[1], Chang Linlin[1], Duan Ying[3†]

(1. *Sports Big Data Center*, *Physical Education College of Zhengzhou University*, *Zhengzhou* 450000, *China*; 2. *School of Mathematics & Statistics*, *Henan University of Science & Technology*, *Luoyang Henan* 471023, *China*; 3. *School of Intelligent Engineering*, *Zhengzhou University of Aeronautics*, *Zhengzhou* 450003, *China*)

Abstract: Linkable ring signatures could avoid double-spending attacks in the blockchain. Lattice-based signatures were quantum-resistant. However, as the number of ring members increased, the size of existing lattice-based linkable ring signatures increased. To solve this problem, a lattice-based linkable ring signatures scheme was proposed. This scheme used queues to implement a special conversion of vector number system, and used lattice-based accumulators to accumulate the public keys of ring members, so that the signature size didn't increase with the number of ring members. And using the rejection sampling theorem, this scheme constructed signatures based on proofs of knowledge on lattices, prevented the signature private key from leaking, and improved the computational efficiency. In the random oracle model, the scheme was proved to be unforgeable, anonymous and linkable. Performance analysis and experimental evaluation show that, this scheme saves time and storage, and the signature size is constant with the increase of ring members.

Key words: lattice; signatures based on proofs of knowledge; accumulators; short linkable ring signatures

0 引言

区块链[1]具有去中心化、开放性、不可窜改性、自治性、匿名性等特点，日前越来越受到业界的推崇。然而区块链技术在安全上还有很多不足，如比特币系统中的匿名性是通过假名实现的，并不是真正的匿名性[2]。针对该问题，很多学者提出改善区块链系统匿名性的方案，环签名[3]便是主流方案之一。在环签名机制下，签名者自发选择多个用户组成环，利用自己的公私钥对及环成员的公钥对消息进行签名，验证者只知道签名出自环中某一个成员，但不能确定签名者真实身份[4]。

对于区块链电子货币系统的双花攻击与区块链电子选举系统的重复投票问题，可链接环签名[5]的可链接性确保签名者不能重复签名，能有效解决区块链的这些问题。文献[6]利用可链接环签名设计了基于智能合约的电子投票系统，确保了投票结果的可信度，解决了投票过程中的安全问题。但是随着环成员的增多，单个可链接环签名的大小也在增大。简短可链接环签名(Short Linkable Ring Signatures, SLRS)[7,8]先使用累加器对公钥环进行累加计算，然后再进行签名，不仅保留了可链接环签名的一些特性，而且随着环成员的增多，单个签名的大小保持不变[9]。文献[9]利用消息编码、Paillier同态加密、简短可链接环签名[7,8]，提出了一个独立平台的安全的区块链投票系统。然而上述这些方案的密码体制均基于传统数学难题，随着量子计算技术的发展，它们的安全性在降低。

基于格的密码体制具有抗量子攻击、运算简单、可并行化、抗量子攻击、存在最坏情况下的随机实例和较好的渐进效率等优点，因而成为后量子时代的研究热点[10]。文献[11]提出了基于格的一次性可链接环签名 L2RS，并将其应用至区块链上的环可信交易(Lattice RingCT v1.0)；在此基础上，文献[12]构造了了可链接环签名 MIMO.L2RS，进一步提出升级版应用协议——Lattice RingCT v2.0，在交易中支持多输入及多输出电子钱包。文献[13]提出了切合实际的格基一次性可链接环签名方案，简单有效，实用性强。针对门罗币的安全问题，文献[14]提出了支持匿名地址[15]的格基可链接环签名。文献[16]利用环上容错学习问题提出了一个可链接环签

收稿日期：2022-02-15；**修回日期：**2022-04-01 **基金项目：**国家自然科学基金资助项目(U1904119)；河南省科技攻关项目(222102210079，212102310264)

作者简介：王杰昌(1985-)，男，河南伊川人，讲师，硕士，主要研究方向为信息安全、区块链；张平(1976-)，男，黑龙江牡丹江人，副教授，硕导，博士，主要研究方向为信息安全与密码学；李杰(1978-)，男，河南禹州人，副教授，硕士，主要研究方向为信息安全；常琳林(1983-)，女，河南项城人，讲师，硕士，主要研究方向为信息安全；段莹(1983-)，女(通信作者)，河南偃师人，副教授，博士，主要研究方向为工业物联网安全(able0607@163.com).

chinaXiv:202205.00088v1

ChinaXiv合作期刊

名方案，密钥尺寸较短，效率较高。文献[10]利用原像抽样和拒绝采样算法构造了一个格上基于身份的可链接环签名方案，提升了用户密钥生成和签名验证的效率。文献[17]利用格密码、消息块共享技术、填充排列技术，提出一种基于格的可链接门限环签名方案，并将其应用至电子投票协议。然而随着环成员个数的增大，这些方案的签名长度也在增大。

为解决上述问题，本文提出格上的简短可链接环签名方案，主要贡献如下：

a)鉴于队列先进先出的特点[18]，利用其实现了向量数制的特殊转换；

b)将 Camenish 和 Stadler 所提出的知识证明签名(Signatures based on Proofs of Knowledge, *SPK*)[19]推广至格上，构造出新的 *SPK*；

c)根据文献[7][8]定义的简短可链接环签名算法，结合格上的累加器[20]，利用拒绝采样定理[21]，构造出格上的简短可链接环签名方案(Lattice-based Short Linkable Ring Signatures, LSLRS)，随着环成员的增加，签名大小保持不变，同时提高了计算效率。

1　预备知识

1.1　基础符号

对于 $b\in\{0,1\}$，用 $\bar{b}$ 表示 $1-b\in\{0,1\}$，矩阵 $\boldsymbol{A}\in\mathbb{Z}^{k\times i}$ 和 $\boldsymbol{B}\in\mathbb{Z}^{k\times j}$ 的拼接表示为 $[\boldsymbol{A}|\boldsymbol{B}]\in\mathbb{Z}^{k\times(i+j)}$，用 $x\xleftarrow{\$}S$ 表示从有限集 S 中均匀随机选择 x，用 $x\xleftarrow{\$}D$ 表示按照分布 D 选择 x。对于正整数 n,q,k,m，n 为安全参数，$q=\tilde{O}(n),k=\lceil\log q\rceil,m=2nk$。对于矩阵 $\boldsymbol{G}=\begin{pmatrix}1\ 2\ 4\ \cdots\ 2^{k-1} & & & \\ & 1\ 2\ 4\ \cdots\ 2^{k-1} & & \\ & & \cdots & \\ & & & 1\ 2\ 4\ \cdots\ 2^{k-1}\end{pmatrix}\in\mathbb{Z}_q^{n\times nk}$，向量 $\boldsymbol{v}=(v_0,\cdots,v_i,\cdots v_{n-1})^{\mathrm{T}}\in\mathbb{Z}_q^n$，有 $\boldsymbol{v}=\boldsymbol{G}\cdot bin(\boldsymbol{v})$，这里 $bin(\boldsymbol{v})\in\{0,1\}^{nk}$ 为向量 $\boldsymbol{v}$ 的二进制表示。

1.2　格上的困难问题

定义 1　$\mathrm{SIVP}_{\boldsymbol{\gamma}}$问题。给定秩为 n 的格 $L=L(\boldsymbol{B})$，找 n 线性无关的向量 $\boldsymbol{v}_1,\cdots,\boldsymbol{v}_n\in L$，使得对任意的 $1\le i\le n$，$\|\boldsymbol{v}_i\|\le\gamma\cdot\lambda_n(L)$，这里 $\gamma\ge1$ 为逼近因子，$\lambda_n(L)$ 为格 L 的逐次最小长度。

定义 2　$\mathrm{SIS}^{\infty}_{n,m,q,\beta}$ 问题[20]。给定均匀随机选择的矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，找到一个非零向量 $\boldsymbol{x}\in\mathbb{Z}^m$ 满足条件 $\|\boldsymbol{x}\|_\infty\le\beta$ 且 $\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{0}\bmod q$。

如果 $m,\beta=poly(n)$，并且 $q>\beta\cdot\tilde{O}(\sqrt{n})$，那么 $\mathrm{SIS}^{\infty}_{n,m,q,\beta}$ 问题至少和最坏情况下的 $\mathrm{SIVP}_{\boldsymbol{\gamma}}$($\gamma=\beta\cdot\tilde{O}(\sqrt{nm})$)问题一样难解。特别地，当 $\beta=1$，$q=\tilde{O}(n),m=2n\lceil\log q\rceil$，$\mathrm{SIS}^{\infty}_{n,m,q,1}$ 问题至少和 $\mathrm{SIVP}_{\tilde{O}(n)}$ 问题一样难解[20]。

1.3　格上的累加器

定义 3　函数族 $\mathcal{H}:\{0,1\}^{nk}\times\{0,1\}^{nk}\to\{0,1\}^{nk}$ 被定义为 $\mathcal{H}=\{H_{\boldsymbol{A}}\mid\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}\}$，这里 $\boldsymbol{A}=[\boldsymbol{A}_0\mid\boldsymbol{A}_1]$，$\boldsymbol{A}_0,\boldsymbol{A}_1\in\mathbb{Z}_q^{n\times nk}$，并且对于任何 $(\boldsymbol{u}_0,\boldsymbol{u}_1)\in\{0,1\}^{nk}\times\{0,1\}^{nk}$，有

$$H_{\boldsymbol{A}}(\boldsymbol{u}_0,\boldsymbol{u}_1)=bin(\boldsymbol{A}_0\cdot\boldsymbol{u}_0+\boldsymbol{A}_1\cdot\boldsymbol{u}_1\bmod q)\in\{0,1\}^{nk}$$

注意 $H_{\boldsymbol{A}}(\boldsymbol{u}_0,\boldsymbol{u}_1)=\boldsymbol{u}\Leftrightarrow\boldsymbol{A}_0\cdot\boldsymbol{u}_0+\boldsymbol{A}_1\cdot\boldsymbol{u}_1=\boldsymbol{G}\cdot\boldsymbol{u}\bmod q$。

引理 1　假设 $\mathrm{SIVP}_{\tilde{O}(n)}$ 问题是难解的，则定义 3 中的函数族 $\mathcal{H}$ 是抗碰撞的。

基于上面定义的格基哈希函数族 $\mathcal{H}$，构造一个默克尔树，具有 $N=2^l$ 个叶子节点，l 为一个正整数，下面为格上累加器[20]的算法：

1)TSetup(n)：抽样 $\boldsymbol{A}\xleftarrow{\$}\mathbb{Z}_q^{n\times m}$，输出 $pp=\boldsymbol{A}$。

2)TAcc$_{\boldsymbol{A}}$(R)：$R=\{\boldsymbol{d}_0\in\{0,1\}^{nk},\cdots,\boldsymbol{d}_{N-1}\in\{0,1\}^{nk}\}$，对每个 $j\in[0,N-1]$，$(j_1,\cdots,j_l)\in\{0,1\}^l$ 为 j 的二进制表示，令 $\boldsymbol{d}_j=\boldsymbol{u}_{j_1,\cdots,j_l}$。深度为 $l=\log N$ 的默克尔树，有 N 个叶子节点 $\boldsymbol{u}_{0,0,\cdots,0},\cdots,\boldsymbol{u}_{1,1,\cdots,1}$，且有如下定义：

①在深度 $i\in\{1,\cdots,l\}$，对于所有的 $(b_1,\cdots,b_i)\in\{0,1\}^i$，节点 $\boldsymbol{u}_{b_1,\cdots,b_i}\in\{0,1\}^{nk}$ 被定义为 $H_{\boldsymbol{A}}(\boldsymbol{u}_{b_1,\cdots,b_i,0},\boldsymbol{u}_{b_1,\cdots,b_i,1})$；

②在深度 0，根节点 $\boldsymbol{u}\in\{0,1\}^{nk}$ 被定义为 $H_{\boldsymbol{A}}(\boldsymbol{u}_0,\boldsymbol{u}_1)$。

该算法输出为累加值 $\boldsymbol{u}$。

3)TWitness$_{\boldsymbol{A}}$($R,\boldsymbol{d}$)：如果 $\boldsymbol{d}\notin R$，返回⊥；否则 $\boldsymbol{d}=\boldsymbol{d}_j$(某个 $j\in[0,N-1]$，这个 j 的二进制表示 $(j_1,\cdots,j_l)$)，输出证据 w 被定义为

$$w=((j_1,\cdots,j_l),(\boldsymbol{u}_{j_1,\cdots,j_{l-1},\bar{j}_l},\cdots,\boldsymbol{u}_{j_1,\bar{j}_2},\boldsymbol{u}_{\bar{j}_1}))\in\{0,1\}^l\times(\{0,1\}^{nk})^l$$

这里 $\boldsymbol{u}_{j_1,\cdots,j_{l-1},\bar{j}_l},\cdots,\boldsymbol{u}_{j_1,\bar{j}_2},\boldsymbol{u}_{\bar{j}_1}$ 可以通过 TAcc$_{\boldsymbol{A}}$(R)算法进行计算得出。

4)TVerify$_{\boldsymbol{A}}$($\boldsymbol{u},\boldsymbol{d},w$)：将给定的证据 w 写成如下形式：

$$w=((j_1,\cdots,j_l),(\boldsymbol{w}_l,\cdots,\boldsymbol{w}_1))\in\{0,1\}^l\times(\{0,1\}^{nk})^l$$

按以下方式递归地计算 $\boldsymbol{v}_l,\boldsymbol{v}_{l-1},\cdots,\boldsymbol{v}_1,\boldsymbol{v}_0\in\{0,1\}^{nk}$：

$$\boldsymbol{v}_l=\boldsymbol{d}$$

$$\forall i\in\{l-1,\cdots,1,0\},\boldsymbol{v}_i=\begin{cases}h_{\boldsymbol{A}}(\boldsymbol{v}_{i+1},\boldsymbol{w}_{i+1}), & 若 j_{i+1}=0\\ h_{\boldsymbol{A}}(\boldsymbol{w}_{i+1},\boldsymbol{v}_{i+1}), & 若 j_{i+1}=1\end{cases}$$

如果 $\boldsymbol{v}_0=\boldsymbol{u}$，返回 1；否则返回 0。

定理 1　假设 $\mathrm{SIVP}_{\tilde{O}(n)}$ 问题是难解的，则格上的累加器是安全的，即对于所有的 PPT 敌手 $\mathcal{A}$：

$$\Pr[pp\leftarrow\mathrm{TSetup}(n);(R,\boldsymbol{d}^*,w^*)\leftarrow\mathcal{A}(pp):$$
$$\boldsymbol{d}^*\notin R\wedge\mathrm{TVerify}_{pp}(\mathrm{TAcc}_{pp}(R),\boldsymbol{d}^*,w^*)=1]=\mathrm{negl}(n)$$

1.4　知识证明签名 SPK

Camenisch 和 Stadler 提出了基于知识证明的签名，简称 *SPK*[8,19]。若证明者想向验证者证明其知道离散对数 $\{(x):y=g^x\bmod n\}$ 的知识，并用这个知识对消息μ进行签名，可通过以下的协议来实现：

证明者：随机选取 $r\in_R\mathbb{Z}_n$，计算

$$\begin{cases}c=H(\mu\|y\|g\|g^r)\\ s=r-cx(\bmod n)\end{cases}$$

，其中 H 为抗碰撞单向哈希函数，

然后将(c, s)传送给验证者。

验证者：检验 $c\overset{?}{=}H(\mu\|y\|g\|g^sy^c)$，若等式成立，验证者接受证明者的证明；否则拒绝。

此处称(c, s)为证明者根据 y 关于 g 的离散对数对消息μ进行的知识证明签名，记为 $SPK\{(x):y=g^x\bmod n\}(\mu)$。

1.5　拒绝采样定理

定理 2　(拒绝采样定理[21]) 集合 $V=\{\boldsymbol{v}\in\mathbb{Z}^m:\|\boldsymbol{v}\|<T\}$ 为 $\mathbb{Z}^m$ 的一个子集，$\mathbb{R}$ 中某个元素 $s=\omega(T\sqrt{\log m})$，概率分布 $h:V\to\mathbb{R}$，则存在常数 $M=O(1)$，使得以下两个算法的输出分布统计距离在 $2^{-\omega(\log m)}/M$ 以内：

算法 A：第一步 $\boldsymbol{v}\xleftarrow{\$}h$，然后 $\boldsymbol{z}\xleftarrow{\$}D^m_{\boldsymbol{v},s}$，最后以 $\min\left(\frac{D^m_s(\boldsymbol{z})}{MD^m_{\boldsymbol{v},s}(\boldsymbol{z})},1\right)$ 的概率输出 $(\boldsymbol{z},\boldsymbol{v})$；

算法 F：第一步 $\boldsymbol{v}\xleftarrow{\$}h$，然后 $\boldsymbol{z}\xleftarrow{\$}D^m_s$，最后以 $1/M$ 的概率输出 $(\boldsymbol{z},\boldsymbol{v})$。

进一步，算法 A 有输出的概率至少为 $1-2^{-\omega(\log m)}/M$。

2　签名定义及安全模型

2.1　签名定义

格上的简短可链接环签名方案包括以下五个 PPT 算法：

1)LSetup(n)：输入安全参数 n，输出公共参数 pp，该参数对所有用户是公开的。

2)LKgen(pp)：输入公共参数 pp，输出公私钥对 (pk,sk)。

3)LSign$_{pp}$(sk,μ,R)：输入签名者的密钥 sk，待签名消息μ，以及环 $R=(pk_0,\cdots,pk_{N-1})$，输出签名 $\sigma_R(M)$，签名包含可链接标签 I。这里 (pk,sk) 为 LKgen(pp)生成的有效的公私钥对，且 $pk\in R$。

4)LVerify$_{pp}$($\mu,R,\sigma_R(\mu)$)：输入消息μ在环 R 上的签名 $\sigma_R(\mu)$，若 $\sigma_R(\mu)$ 是有效的，本算法输出 1；否则输出 0。

5)LLink($\sigma_R(\mu_1),\sigma_R(\mu_2)$)：输入签名 $\sigma_R(\mu_1),\sigma_R(\mu_2)$，若 $I_1=I_2$，则输出 Linked；否则输出 Unlinked。

2.2　安全模型

2.2.1 不可伪造性

不可伪造性游戏如下：

chinaXiv:202205.00088v1

ChinaXiv合作期刊

1)初始化：系统运行 LSetup 得到公共参数，并将公共参数发送给敌手 $\mathcal{A}$。

2)询问阶段：敌手 $\mathcal{A}$ 可以进行多项式次访问随机预言机。

3)伪造阶段：敌手 $\mathcal{A}$ 输出 (μ^*,R^*,σ^*)，若满足以下条件。

①敌手进行第 j 次公钥询问，公钥预言机 $\mathcal{PO}$ 生成公私钥对 (pk_j,sk_j)，将公钥加入环中，并返回公钥 pk_j；

②敌手输入 (j,μ,R) 进行签名询问，若 (pk_j,sk_j) 由 $\mathcal{PO}$ 生成且 $pk_j\in R$，则签名预言机 $\mathcal{SO}$ 输出与 (j,μ,R) 相对应的签名 $\sigma_R(\mu)$；否则输出⊥；

③敌手输入 pk_j 询问其对应的私钥，私钥预言机 $\mathcal{CO}$ 返回 sk_j；

④ $(\cdot,\mu^*,R^*)$ 从未被敌手询问过，环 R^* 中的公钥均为 $\mathcal{PO}$ 生成，且其对应的私钥均未被询问过。

则敌手 $\mathcal{A}$ 赢得不可伪造性游戏，敌手赢得游戏的优势定义为

$$Adv_{\mathcal{A}}^{F}=\Pr[pp\leftarrow LSetup(1^n);(\mu^*,R^*,\sigma^*)\leftarrow\mathcal{A}^{\mathcal{PO},\mathcal{SO},\mathcal{CO}}(pp):\\ \text{LVerify}_{pp}(\mu^*,R^*,\sigma^*)=1]$$

定义 4　对于任意多项式时间敌手 $\mathcal{A}$，$Adv_{\mathcal{A}}^{F}=\text{negl}(n)$，则称该简短可链接环签名是不可伪造的。

2.2.2 匿名性

匿名性游戏如下：

1)初始化：挑战者 $\mathcal{B}$ 运行算法 LSetup 得到公共参数 pp，并且运行算法 LKgen 生成公私钥对 $(\boldsymbol{d}_i,\boldsymbol{x}_i)$，将公钥加入环中，然后将环 $R=(\boldsymbol{d}_0,\cdots,\boldsymbol{d}_{N-1})$ 和公共参数 pp 发送给敌手 $\mathcal{A}$。

2)询问阶段：敌手 $\mathcal{A}$ 可以进行多项式次访问预言机。

3)挑战阶段：敌手 $\mathcal{A}$ 挑选待签消息 $\mu\in\{0,1\}^*$，以及任意两个公钥 $\boldsymbol{d}_{i_0},\boldsymbol{d}_{i_1}\in R$ 进行签名询问，挑战者随机选择 $b\in\{0,1\}$ 并利用 $\boldsymbol{d}_{i_b}$ 对应的私钥 x_{i_b}，运行 LSign 对消息 μ 进行签名，将生成的签名 $\sigma_R(\mu)$ 返回给敌手 $\mathcal{A}$。

4)猜测阶段：敌手 $\mathcal{A}$ 输出 b^* 作为对签名者身份的猜测，若 $b^*=b$，则敌手获胜。

敌手 $\mathcal{A}$ 在匿名性游戏中获胜的的优势定义为

$$Adv_{\mathcal{A}}^{Ano}=\left|\Pr[b^*=b]-\frac{1}{2}\right|$$

定义 5　对于任意多项式时间敌手 $\mathcal{A}$，$Adv_{\mathcal{A}}^{Ano}=\text{negl}(n)$，则称该签名方案是匿名的。

2.2.3 可链接性

可链接性游戏如下：

1)初始化：挑战者 $\mathcal{B}$ 运行算法 LSetup 得到公共参数 pp，并且运行算法 LKgen 生成公私钥对 $(\boldsymbol{d}_i,\boldsymbol{x}_i)$，将公钥加入环中，然后将环 $R=(\boldsymbol{d}_0,\cdots,\boldsymbol{d}_{N-1})$ 和公共参数 pp 发送给敌手 $\mathcal{A}$。

2)询问阶段：敌手 $\mathcal{A}$ 可以进行多项式次访问预言机。

3)伪造阶段：敌手 $\mathcal{A}$ 给出两签名 $(\mu_1,R_1,\sigma_{R_1}(\mu_1))$，$(\mu_2,R_2,\sigma_{R_2}(\mu_2))$，签名 $\sigma_{R_1}(\mu_1),\sigma_{R_2}(\mu_2)$ 中分别包含相应的可链接标签 I_1,I_2，若满足以下条件：

① $\text{LVerify}_{pp}(\mu_i,R_i,\sigma_{R_i}(\mu_i))=1,i\in\{1,2\}$；

② $\text{LLink}(\sigma_{R_1}(\mu_1),\sigma_{R_2}(\mu_2))=\text{Unlinked}$，即 $I_1\neq I_2$；

③敌手 $\mathcal{A}$ 未发起过 $(\mu_1,R_1),(\mu_2,R_2)$ 的签名询问；

④环 R_1,R_2 中任一用户的公钥均由挑战者给出；

⑤敌手 $\mathcal{A}$ 发起私钥询问的次数少于两次(敌手 $\mathcal{A}$ 至多拥有一个用户的私钥)。

则敌手 $\mathcal{A}$ 赢得可链接性游戏，敌手 $\mathcal{A}$ 赢得游戏的优势定义为 $Adv_{\mathcal{A}}^{L}=\Pr[\mathcal{A}\ wins]$。

定义 6　对于任意多项式时间敌手 $\mathcal{A}$，$Adv_{\mathcal{A}}^{L}$ 是可忽略的，则称该简短可链接环签名是可链接的。

3　格上的简短可链接环签名

Camenisch 和 Stadler[19]首先提出了基于知识证明的签名，根据离散对数 x 这一知识对消息 μ 进行了知识证明签名，即 $\sigma=SPK\{(x):y=g^x\bmod n\}(\mu)$。文献[7]中，Tsang 和 Wei 使用了基于知识证明的签名，如根据知识 (w,y_s,x) 对消息 M 进行的知识证明签名，即 $\sigma=SPK\{(w,y_s,x):(y_s,x)\in\mathbb{R}\wedge f(w,y_s)=v\wedge\tilde{y}=\theta_d(x)\}(M)$，并结合累加器，提出了简短可链接环签名。文献[7,8]中的简短可链接环签名，均是先使用累加器对环中公钥进行累加，然后再进行基于知识证明的签名。随着环成员的增多，可链接环签名大小随之增大，而简短可链接环签名的大小保持不变，同时保留不可伪造性、匿名性、可链接性等优点[9]。但上述累加器、SPK 及其构造的简短可链接环签名，均基于传统的数学难题，且目前仅有学者提出的格上的可链接环签名方案[10,11]，还没有格上的简短可链接环签名方案。因此本文根据简短可链接环签名[7,8]的构造，先利用格上的累加器[20]对环中公钥进行累加，然后依据文献[7,8,19]的算法提出格上的 SPK，最终构造出格上的简短可链接环签名 LSLRS。

LSLRS 方案中有 $N=2^l$ 个环成员，参数 n,m,q,k 在预备知识中已定义。LSLRS 包含五个算法(LSetup, LKgen, LSign_{pp}, LVerify_{pp}, LLink)，具体描述如下：

1)LSetup(n)：输入安全参数 n，从 $\mathbb{Z}_q^{n\times m}$ 中均匀随机抽样得到 $\boldsymbol{A}$，选取抗碰撞的单向哈希函数：$H_{\boldsymbol{A}}\in\mathcal{H}:\{0,1\}^{nk}\times\{0,1\}^{nk}\to\{0,1\}^{nk}$，$H_1:\mathbb{Z}_q^{n\times m}\times\{0,1\}^m\to\mathbb{Z}_q$，$H_2:\{0,1\}^l\times(\{0,1\}^{nk})^l\to\mathbb{Z}_q$，$H_3:\{0,1\}^*\times\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^n\times\{0,1\}^{nk}\times\mathbb{Z}_q\to\mathbb{Z}_q$，输出公共参数 $pp=(\boldsymbol{A},H_{\boldsymbol{A}},H_1,H_2,H_3)$。

2)LKgen(pp)：输入 pp，从 $\{0,1\}^m$ 中均匀随机选择 $\boldsymbol{x}_i,i\in[0,N-1]$，分别计算 $\boldsymbol{d}_i=bin(\boldsymbol{A}\cdot\boldsymbol{x}_i\bmod q)$，$\boldsymbol{d}_i\in\{0,1\}^{nk}$ (这里算法 $bin(\ )$ 的具体实现见 3.1 节)，输出公私钥对 $(sk_i,pk_i)=(\boldsymbol{x}_i,\boldsymbol{d}_i)$，$i\in[0,N-1]$。

3)$\text{LSign}_{pp}(sk,\ \mu,\ R)$：输入环 $R=(\boldsymbol{d}_0,\cdots,\boldsymbol{d}_{N-1})$，$\boldsymbol{d}_i\in\{0,1\}^{nk},i\in[0,N-1]$，签名私钥 $sk=\boldsymbol{x}\in\{0,1\}^m$，其对应的公钥为

$$pk=\boldsymbol{d}=bin(\boldsymbol{A}\cdot\boldsymbol{x}\bmod q)\in R \tag{1}$$

按以下步骤生成消息 $\mu\in\{0,1\}^*$ 的签名 σ：

①　计算可链接标签

$$I=H_1(\boldsymbol{A},\boldsymbol{x}) \tag{2}$$

②运行算法 $\text{TAcc}_{\boldsymbol{A}}(R)$，输出环 R 中所有环成员公钥的累加值

$$\boldsymbol{u}=H_{\boldsymbol{A}}(\boldsymbol{u}_0,\boldsymbol{u}_1)\in\{0,1\}^{nk} \tag{3}$$

③运行算法 $\text{TWitness}_{\boldsymbol{A}}(R,\ \boldsymbol{d})$得到证据

$$w=((j_1,\cdots,j_l),(\boldsymbol{w}_l,\cdots,\boldsymbol{w}_1))\in\{0,1\}^l\times(\{0,1\}^{nk})^l \tag{4}$$

④计算知识证明签名

$$\begin{aligned}&SPK\{(w,\boldsymbol{d},\boldsymbol{x}):\\&w=((j_1,\cdots,j_l),(\boldsymbol{u}_{j_1,\cdots,j_{l-1},\bar{j}_l},\cdots,\boldsymbol{u}_{j_1,\bar{j}_2},\boldsymbol{u}_{\bar{j}_1}))\wedge\\&\boldsymbol{d}=bin(\boldsymbol{A}\cdot\boldsymbol{x}\bmod q)\}(\mu)\end{aligned} \tag{5}$$

将 Camenisch 和 Stadler 的 SPK 推广至格上，同时利用拒绝采样定理，构造格上的知识证明签名：

证明者(即签名者)：按照分布 D_s^m 随机选择 $\boldsymbol{r}\in\{0,1\}^m$，分别进行如下计算：

$$W=H_2(w) \tag{6}$$

$$\boldsymbol{c}=bin(\boldsymbol{A}\cdot\boldsymbol{r}\bmod q) \tag{7}$$

$$z=H_3(\mu,\boldsymbol{A},\boldsymbol{G}\cdot\boldsymbol{d},\boldsymbol{c},W) \tag{8}$$

$$\boldsymbol{k}=\boldsymbol{r}-z\cdot\boldsymbol{x}(\bmod q) \tag{9}$$

然后将 $(W,\boldsymbol{c},z,\boldsymbol{k})$ 传送给验证者，根据拒绝采样定理，发送成功的概率为 $\min\left(\frac{D_s^m(\boldsymbol{k})}{MD_{-z\boldsymbol{x},s}^m(\boldsymbol{k})},1\right)$，如果发送失败，则重新计算后再发送；

验证者：检验

$$z\overset{?}{=}H_3(\mu,\boldsymbol{A},z^{-1}\cdot\boldsymbol{G}\cdot\boldsymbol{c}-z^{-1}\cdot\boldsymbol{A}\cdot\boldsymbol{k}(\bmod q),\boldsymbol{c},W) \tag{10}$$

若上式成立，验证者接受证明；否则拒绝。

$(W,\boldsymbol{c},z,\boldsymbol{k})$ 为证明者(即签名者)根据知识 $(w,\boldsymbol{d},\boldsymbol{x})$ 对消息μ进行的签名，即

chinaXiv:202205.00088v1

ChinaXiv合作期刊

$$SPK\{(w,\boldsymbol{d},\boldsymbol{x}): w=((j_1,\cdots,j_l),(\boldsymbol{u}_{j_1,\cdots,j_{l-1},\bar{j}_l},\cdots,\boldsymbol{u}_{j_1,\bar{j}_2},\boldsymbol{u}_{\bar{j}_1}))\wedge \boldsymbol{d}=bin(\boldsymbol{A}\cdot\boldsymbol{x} \bmod q)\}(\mu)=(W,\boldsymbol{c},z,\boldsymbol{k}) \tag{11}$$

⑤输出格上的简短可链接环签名

$$\sigma_R(\mu)=(\boldsymbol{u},I,SPK)=(\boldsymbol{u},I,W,\boldsymbol{c},z,\boldsymbol{k}) \tag{12}$$

4)LVerify$_{pp}$(μ, R, $\sigma_R(\mu)$)：输入签名消息 μ，环 $R=(\boldsymbol{d}_0,\cdots,\boldsymbol{d}_{N-1})$，以及签名 $\sigma_R(\mu)=(\boldsymbol{u},I,SPK)$；从 R 中任意选取一个 $\boldsymbol{d}_j, j\in[0,N-1]$，计算 $\mathrm{TAcc}_{\boldsymbol{A}}(R)\to\boldsymbol{u}'$，验证 $\boldsymbol{u}\overset{?}{=}\boldsymbol{u}'$，并且验证式(11)的有效性，若都验证通过，则输出 1；否则输出 0。

5)LLink($\sigma_R(\mu_1),\sigma_R(\mu_2)$)：给定两个签名 $\sigma_R(\mu_1),\sigma_R(\mu_2)$，提取它们的可链接标签，若 $I_1=I_2$，则输出 Linked；否则输出 Unlinked。

3.1　算法 $bin(\,)$

设 $\boldsymbol{v}\in\mathbb{Z}_q^n$，有 $\boldsymbol{v}=(v_0,v_1,\cdots,v_{n-1})^{\mathrm{T}}$，$v_i\in\mathbb{Z}_q, i\in[0,n-1]$，$bin(\boldsymbol{v})\in\{0,1\}^{nk}$ 为向量 $\boldsymbol{v}$ 的二进制表示。$\boldsymbol{v}=\boldsymbol{G}\cdot bin(\boldsymbol{v})$，十进制数 v_i 应转换为具有特殊写法的二进制数(与正常的二进制数写法顺序相反，从最低位数开始写起，且自上而下书写，依次写到最高位数而止)，然后自上而下依次书写 $v_0,v_1,\cdots,v_{n-1}$ 所对应的特殊写法二进制数，最终得到向量 $bin(\boldsymbol{v})$。由于队列具有先进先出的特点，这里可通过队列实现 $\boldsymbol{v}$ 的数制转换，其算法的具体实现过程如下所示。

输入：十进制向量 $\boldsymbol{v}$。

输出：$bin(\boldsymbol{v})$。

```
void coversion(int N)
{//对于任一十进制数，输出其对应的二进制数
  InitQueue(Q);        //初始化空队列 Q
  while (log₂N>=2)
  {
      EnQueue(Q, N%2);  /*调用函数 EnQueue()，将 N 与 2 求余得到的二进制数加入队列 Q */
      N=N/2;
  }
  while (!QueueEmpty(Q))  //当队列 Q 非空时，循环
  {
      DeQueue(Q, e);        /*调用函数 DeQueue()，弹出队列 Q 的队头元素 e */
      count<<e;
  }
}
void main()
{//将 n 维向量 v 转换为其对应的二进制向量 bin(v)
  int v[n];
  for (i=0; i<n; i++)
     coversion(int v[i]);   /*调用函数 coversion()，将十进制数 v[i]转换为二进制数*/
}
```

4　安全性分析

4.1　正确性

格上累加器的正确性文献[20]中已进行了论证，这里主要论证知识签名证明的正确性：

$$\begin{aligned}
&H_3(\mu,\boldsymbol{A},z^{-1}\cdot\boldsymbol{G}\cdot\boldsymbol{c}-z^{-1}\cdot\boldsymbol{A}\cdot\boldsymbol{k}(\bmod q),\boldsymbol{c},W)=\\
&H_3(\mu,\boldsymbol{A},z^{-1}\cdot(\boldsymbol{G}\cdot bin(\boldsymbol{A}\cdot\boldsymbol{r} \bmod q)-\boldsymbol{A}\cdot\boldsymbol{k}(\bmod q)),\boldsymbol{c},W)=\\
&H_3(\mu,\boldsymbol{A},z^{-1}\cdot(\boldsymbol{A}\cdot\boldsymbol{r}-\boldsymbol{A}\cdot\boldsymbol{k}(\bmod q)),\boldsymbol{c},W)=\\
&H_3(\mu,\boldsymbol{A},\boldsymbol{A}\cdot z^{-1}\cdot(\boldsymbol{r}-\boldsymbol{k}) \bmod q,\boldsymbol{c},W)=\\
&H_3(\mu,\boldsymbol{A},\boldsymbol{A}\cdot z^{-1}\cdot z\cdot\boldsymbol{x} \bmod q,\boldsymbol{c},W)=\\
&H_3(\mu,\boldsymbol{A},\boldsymbol{A}\cdot\boldsymbol{x} \bmod q,\boldsymbol{c},W)=\\
&H_3(\mu,\boldsymbol{A},\boldsymbol{G}\cdot\boldsymbol{d},\boldsymbol{c},W)=z
\end{aligned}$$

4.2　不可伪造性

定理 3　如果 $\mathrm{SIVP}_{\tilde{O}(n)}$ 问题是困难的，那么在随机预言机模型下，格上的简短可链接环签名是不可伪造的。

证明：　在随机预言机模型下，假设敌手 $\mathcal{A}$ 以 ε 的优势赢得不可伪造性游戏，那么一定存在模拟器 $\mathcal{B}$ 或者攻破格上累加器的安全性，或者以不可忽略的优势解决一个 $\mathrm{SIS}_{n,m,q,1}^{\infty}$ 问题实例。

为达到目的，$\mathcal{B}$ 将公共参数 $(\boldsymbol{A},H_{\boldsymbol{A}},H_1,H_2)$ 发送给 $\mathcal{A}$，在游戏期间，$\mathcal{B}$ 诚实地回答 $\mathcal{A}$ 的公钥询问，并将公钥 $pk=bin(\boldsymbol{A}\cdot\boldsymbol{x} \bmod q)$ 返回给 $\mathcal{A}$。在每次公钥询问中，$\mathcal{B}$ 秘密保留其选择的私钥 $sk=\boldsymbol{x}\in\{0,1\}^m$。掌握所有的私钥，$\mathcal{B}$ 就能回答所有的私钥询问以及签名询问。

游戏结束时，$\mathcal{A}$ 输出通过验证的 (μ^*,R^*,σ^*)，并且 $\mathcal{A}$ 从未询问过环 R^* 成员的私钥，同时也未对 $(\cdot,\mu^*,R^*)$ 进行过签名询问。这里 $R^*=(pk_{i_1},\cdots,pk_{i_{|R^*|}})$ 为一组二进制向量 $(\boldsymbol{d}_0,\cdots,\boldsymbol{d}_{|R^*|-1})$，$\sigma^*=(\boldsymbol{u}^*,I^*,W^*,\boldsymbol{c}^*,z^*,\boldsymbol{k}^*)$，$\boldsymbol{u}^*=\mathrm{TAcc}_{\boldsymbol{A}}(R^*)$。

设 $H_3(\,)$ 为随机预言机，敌手 $\mathcal{A}$ 至多进行 q_H 次哈希询问，根据分叉引理[22]，$\mathcal{A}$ 能以 $(1-e^{-1})\dfrac{\varepsilon}{q_H}$ 的概率输出两个有效的签名 $(\boldsymbol{u}^*,I^*,W^*,\boldsymbol{c}^*,z^*,\boldsymbol{k}^*)$ 和 $(\boldsymbol{u}^*,I^*,W^*,\boldsymbol{c}^*,z_0{}^*,\boldsymbol{k}_0{}^*)$，其中 $z^*\neq z_0^*$。

根据签名机制，模拟器 $\mathcal{B}$ 可得到方程组

$$\begin{cases}\boldsymbol{k}^*=\boldsymbol{r}^*-z^*\cdot\boldsymbol{x}^*(\bmod q)\\ \boldsymbol{k}_0{}^*=\boldsymbol{r}^*-z_0{}^*\cdot\boldsymbol{x}^*(\bmod q)\end{cases}$$

两式相减可计算出

$$\boldsymbol{x}^*=(z_0^*-z^*)^{-1}(\boldsymbol{k}^*-\boldsymbol{k}_0^*) \bmod q$$

然后可计算出

$$\boldsymbol{d}^*=bin(\boldsymbol{A}\cdot\boldsymbol{x}^* \bmod q)$$

进一步根据算法 $\mathrm{TWitness}_{\boldsymbol{A}}(R^*,d^*)$ 可得到 w^*。

最终 $\mathcal{B}$ 得以提取知识 $(w^*,\boldsymbol{d}^*,\boldsymbol{x}^*)$，这里 $w^*=((j^*{}_1,\cdots,j^*{}_l),(\boldsymbol{w}^*{}_l,\cdots,\boldsymbol{w}^*{}_1))$，而 $(j^*{}_1,\cdots,j^*{}_l)\in\{0,1\}^l$ 是某个下标 $j^*\in\{0,\cdots,|R^*|-1\}$ 的二进制展开，同时满足

$$\begin{cases}\boldsymbol{G}\cdot\boldsymbol{d}^*=\boldsymbol{A}\cdot\boldsymbol{x}^* \bmod q\\ \mathrm{TVerify}_{\boldsymbol{A}}(\boldsymbol{u}^*,\boldsymbol{d}^*,w^*)=1\end{cases} \tag{13}$$

此时，分两种情况讨论：

1) $\boldsymbol{d}^*\notin R^*=(\boldsymbol{d}_0,\cdots,\boldsymbol{d}_{|R^*|-1})$，则上面的 $\mathrm{TVerify}_{\boldsymbol{A}}(\boldsymbol{u}^*,\boldsymbol{d}^*,w^*)=1$ 就意味着 $\mathcal{B}$ 可以用 $(\boldsymbol{d}^*,R^*,\boldsymbol{u}^*)$ 攻破格上累加器的安全性。

2) $\boldsymbol{d}^*\in R^*=(\boldsymbol{d}_0,\cdots,\boldsymbol{d}_{|R^*|-1})$，所以 $\boldsymbol{d}^*=\boldsymbol{d}_{j^*}=pk_{j^*}$，提取的知识 $(\boldsymbol{d}_{j^*},\boldsymbol{x}^*)$ 满足

$$\boldsymbol{G}\cdot\boldsymbol{d}_{j^*}=\boldsymbol{A}\cdot\boldsymbol{x}^* \bmod q \tag{14}$$

回忆一下 sk_{j^*} 为在某次公钥询问中模拟器 $\mathcal{B}$ 选择的向量 $\boldsymbol{x}_{j^*}\in\{0,1\}^m$，满足

$$\boldsymbol{G}\cdot\boldsymbol{d}_{j^*}=\boldsymbol{A}\cdot\boldsymbol{x}_{j^*} \bmod q \tag{15}$$

由于敌手 $\mathcal{A}$ 不能询问用户 j^* 的私钥，所以有 1/2 的概率 $\boldsymbol{x}_{j^*}\neq\boldsymbol{x}^*$。式(14)和(15)两式相减可得 $\boldsymbol{A}\cdot(\boldsymbol{x}_{j^*}-\boldsymbol{x}^*)=\boldsymbol{0} \bmod q$，进而可得到 $\mathrm{SIS}_{n,m,q,1}^{\infty}$ 问题的一个有效解 $\boldsymbol{\omega}=\boldsymbol{x}_{j^*}-\boldsymbol{x}^*\in\{-1,0,1\}^m$。

从以上两种情况的讨论可知，若敌手 $\mathcal{A}$ 伪造签名成功，则模拟器 $\mathcal{B}$ 要么破坏格上累加器的安全性，要么解决一个 $\mathrm{SIS}_{n,m,q,1}^{\infty}$ 问题实例。这显然均与 $\mathrm{SIVP}_{\tilde{O}(n)}$ 问题困难假设相矛盾，定理得证。

4.3　匿名性

定理 4　本方案具备匿名性。

证明：　通过挑战者 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 间的匿名性游戏进行证明，Game$_0$ 模拟 $\mathcal{B}$ 利用 $\boldsymbol{d}_{i_0}$ 对应的私钥 $\boldsymbol{x}_{i_0}$ 进行签名，Game$_1$ 模拟 $\mathcal{B}$ 利用 $\boldsymbol{d}_{i_1}$ 对应的私钥 $\boldsymbol{x}_{i_1}$ 进行签名，若敌手 $\mathcal{A}$ 对两个签名的概率分布不可区分，那么本方案满足匿名性。

Game$_0$：

1) $\mathcal{B}$ 输入安全参数 n，从 $\mathbb{Z}_q^{n\times m}$ 中均匀随机抽样得到 $\boldsymbol{A}$，选取抗碰撞单向哈希函数：$H_{\boldsymbol{A}}\in\mathcal{H}$，$H_1$，$H_2$，$H_3$，输出这些公共参数；然后从 $\{0,1\}^m$ 中均匀随机选择 $\boldsymbol{x}_i, i\in[0,N-1]$，分别计算 $\boldsymbol{d}_i=bin(\boldsymbol{A}\cdot\boldsymbol{x}_i \bmod q)$，$\boldsymbol{d}_i\in\{0,1\}^{nk}$，加入环 R，保留私钥

chinaXiv:202205.00088v1

ChinaXiv合作期刊

$\boldsymbol{x}_i, i \in [0, N-1]$，输出环 $R = (\boldsymbol{d}_0, \cdots, \boldsymbol{d}_{N-1})$。

2)敌手 $\mathcal{A}$ 将待签名消息 $\mu \in \{0,1\}^*$，环 $R = (\boldsymbol{d}_0, \cdots, \boldsymbol{d}_{N-1})$，以及环中任意两个公钥 $\boldsymbol{d}_{i_0}, \boldsymbol{d}_{i_1} \in R$ 发送给 $\mathcal{B}$；$\mathcal{B}$ 选取 $b=0$ 即选取 $\boldsymbol{d}_{i_0}$ 对应的私钥 $\boldsymbol{x}_{i_0}$ 进行签名。

3) $\mathcal{B}$ 运行算法 $\mathrm{LSign}_{pp}(\boldsymbol{x}_{i_0}, \mu, R)$，利用拒绝采样定理，生成签名 $\sigma_R(\mu) = (\boldsymbol{u}, I, W, \boldsymbol{c}, z, \boldsymbol{k})$，并将其返回给敌手 $\mathcal{A}$。

4)敌手 $\mathcal{A}$ 收到签名后给出对 b 的猜测。

Game₁：

Game₁ 与 Game₀ 的不同在于 $\mathcal{B}$ 选取 $b=1$ 即选取 $\boldsymbol{d}_{i_1}$ 对应的私钥 $\boldsymbol{x}_{i_1}$，运行签名算法 $\mathrm{LSign}_{pp}(\boldsymbol{x}_{i_1}, \mu, R)$，利用拒绝采样定理生成 $\sigma_R^*(\mu) = (\boldsymbol{u}, I^*, W^*, \boldsymbol{c}^*, z^*, \boldsymbol{k}^*)$，将其返回给敌手 $\mathcal{A}$，敌手 $\mathcal{A}$ 给出对 b 的猜测，其余部分均与 Game₀ 相同。

Game₀ 与 Game₁ 生成的签名分别为 $\sigma_R(\mu)$ 与 $\sigma_R^*(\mu)$，因为 $\sigma_R(\mu)$ 与 $\sigma_R^*(\mu)$ 均是利用拒绝采样定理得到的，故两个签名的分布统计距离可忽略不计，所以两者是不可区分的，因此敌手 $\mathcal{A}$ 在匿名性游戏中获胜的优势是可忽略的，本方案满足匿名性。

4.4　可链接性

定理 5　若本方案是不可伪造的，在随机预言机模型下，对于任意多项式时间敌手 $\mathcal{A}$，本方案签名满足可链接性。

证明：　根据可链接性的定义，假设敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 赢得定义 6 中的游戏，则敌手 $\mathcal{A}$ 将与挑战者 $\mathcal{B}$ 进行如下交互：

1) $\mathcal{B}$ 输入安全参数 n，从 $\mathbb{Z}_q^{n\times m}$ 中均匀随机抽样得到 $\boldsymbol{A}$，选取抗碰撞单向哈希函数：$H_{\boldsymbol{A}} \in \mathcal{H}$，输出这些公共参数；然后从 $\{0,1\}^m$ 中均匀随机选择 $\boldsymbol{x}_i, i \in [0, N-1]$，分别计算 $\boldsymbol{d}_i = bin(\boldsymbol{A} \cdot \boldsymbol{x}_i \bmod q)$，$\boldsymbol{d}_i \in \{0,1\}^{nk}$，加入环 R，保留私钥 $\boldsymbol{x}_i, i \in [0, N-1]$，输出环 $R = (\boldsymbol{d}_0, \cdots, \boldsymbol{d}_{N-1})$。

2)敌手 $\mathcal{A}$ 可以进行多项式次的访问预言机，包括哈希询问、私钥询问及签名询问，$\mathcal{B}$ 将询问结果返回给 $\mathcal{T}_1$。

①私钥询问：$\mathcal{A}$ 可以选择 $\boldsymbol{d} \in R$ 进行询问，$\mathcal{B}$ 将其对应的私钥 $\boldsymbol{x}$ 返回给 $\mathcal{A}$。

②哈希询问：

a) H_1 询问：$\mathcal{A}$ 可以利用私钥 $\boldsymbol{x}$ 进行询问，$\mathcal{B}$ 将 I 返回给 $\mathcal{A}$；

b) H_2 询问：$\mathcal{A}$ 可以选择 $\boldsymbol{d}$ 的 w 进行询问，$\mathcal{B}$ 将 W 返回给 $\mathcal{A}$；

c) H_3 询问：$\mathcal{A}$ 可以选择 $\mu \in \{0,1\}^*$，及 $\boldsymbol{d} \in R$ 进行询问，$\mathcal{B}$ 将 z 返回给 $\mathcal{A}$。

③签名询问：$\mathcal{A}$ 选择环 $R = (\boldsymbol{d}_0, \cdots, \boldsymbol{d}_{N-1})$，$\mu \in \{0,1\}^*$，及 $\boldsymbol{d} \in R$ 进行询问，$\mathcal{B}$ 执行算法 $\mathrm{LSign}_{pp}(sk, \mu, R)$，用 $\boldsymbol{d}$ 对应的私钥 $\boldsymbol{x}$ 进行签名，生成 $\sigma_R(\mu)$ 并返回给 $\mathcal{A}$。

3)敌手 $\mathcal{A}$ 输出两个签名 $\sigma_{R_1}(\mu_1) = (\boldsymbol{u}_1, I_1, W_1, \boldsymbol{c}_1, z_1, \boldsymbol{k}_1)$ 及 $\sigma_{R_2}(\mu_2) = (\boldsymbol{u}_2, I_2, W_2, \boldsymbol{c}_2, z_2, \boldsymbol{k}_2)$。

假设敌手 $\mathcal{A}$ 能在仅持有一个私钥的情况下以不可忽略的优势 ε 生成两个环签名 $\sigma_{R_1}(\mu_1), \sigma_{R_2}(\mu_2)$，并且 $\mathrm{LVerify}_{pp}(\mu_i, R_i, \sigma_{R_i}(\mu_i)) = 1, i \in \{1,2\}$，因为本文提出的简短可链接环签名具有不可伪造性，所以只有当敌手 $\mathcal{A}$ 诚实地按签名机制生成 $\sigma_{R_1}(\mu_1), \sigma_{R_2}(\mu_2)$ 时，这两个签名才能通过验证返回 1。

另一方面，本文有 $I_1 = H_1(\boldsymbol{A}, \boldsymbol{x}_1)$，$I_2 = H_1(\boldsymbol{A}, \boldsymbol{x}_2)$，因为敌手 $\mathcal{A}$ 仅拥有一个私钥，则有 $\boldsymbol{x}_1 = \boldsymbol{x}_2$，在询问随机预言机 $H_1(\cdot,\cdot)$ 时，相同的询问会有相同的回应，此时有 $I_1 = I_2$，则 $\mathrm{LLink}(\sigma_{R_1}(\mu_1), \sigma_{R_2}(\mu_2)) = \mathrm{Linked}$。这与假设相矛盾，所以敌手 $\mathcal{A}$ 的优势是可忽略的。定理得证。

5　性能分析与实验评估

5.1　性能分析

汤永利等的方案[10]及 L2RS [11]均为格上的可链接环签名方案，本方案 LSLRS 将与这两个方案在时间开销和存储开销方面分别进行对比分析。

三种方案的时间开销对比如表 1 所示，统一使用 N 代表环成员个数，统一使用 T_{H} 代表方案中的各种哈希运算的单步平均耗时(除了本方案的 $H_{\boldsymbol{A}}$)，使用 T_{TG}、T_{SP}、T_{SD}、T_{LHL}、T_{MUL}、T_{bin}、T_{TAcc}、T_{TWitness} 分别表示陷门生成算法[23]、原像抽样算法[23]、高斯抽样算法[23]、剩余哈希引理[11]、矩阵向量乘法、$bin(\,)$ 算法、$\mathrm{TAcc}_{\boldsymbol{A}}()$算法、$\mathrm{TWitness}_{\boldsymbol{A}}()$算法的单步平均耗时，这些运算耗时相对较多，主要以这些运算衡量方案的时间开销，忽略矩阵加减等耗时相对较少的运算。从系统创建(Setup)、用户密钥生成(Key generate)、签名生成(Sign)、签名验证(Verify)所消耗的时间进行分析，其中 log 的底数为 2。

在系统创建阶段，汤永利等的方案[10]是基于身份的可链接环签名，需要运用陷门生成算法生成系统主密钥，故其该阶段的时间开销主要为 T_{TG}，L2RS[11]及本方案非基于身份的签名，没有这部分的时间开销。在用户密钥生成阶段，因需要生成 N 对公私钥，本文 LSLRS 需执行 N 次矩阵向量乘法和 N 次 $bin(\,)$ 算法，$T_{\mathrm{bin}} = O(\max \log v_i)$，$T_{\mathrm{MUL}} = O(nm)$，显然 $T_{\mathrm{bin}} < T_{\mathrm{MUL}}$；汤永利方案[10]需要 N 次的哈希运算和 N 次的原像抽样算法，L2RS[11]需要 N 次的矩阵向量乘法和 N 次的剩余哈希引理算法。在签名生成阶段，本方案 LSLRS 需要执行 3 次哈希运算、一次 $\mathrm{TAcc}_{\boldsymbol{A}}()$算法、一次 $\mathrm{TWitness}_{\boldsymbol{A}}()$算法、一次高斯抽样算法、一次矩阵向量乘法、及一次 $bin(\,)$ 算法，其中 $H_{\boldsymbol{A}}$ 的时间复杂度为 $T_{H_{\boldsymbol{A}}} = 2T_{\mathrm{MUL}} + T_{\mathrm{bin}} = O(nm) + O(\max \log v_i) = O(nm)$，$T_{\mathrm{TAcc}} = (N-1)T_{H_{\boldsymbol{A}}} = (N-1)\cdot O(nm) = (N-1)T_{\mathrm{MUL}}$，$T_{\mathrm{TWitness}} = O(l^2) = O(\log^2 N)$，显然 $T_{\mathrm{TWitness}} < T_{\mathrm{MUL}}$，该阶段本方案的时间开销为 $3T_{\mathrm{H}} + N \cdot T_{\mathrm{MUL}} + T_{\mathrm{TWitness}} + T_{\mathrm{bin}} + T_{\mathrm{SD}}$；汤永利方案[10]需要执行 N+1 次的哈希运算、2N+1 次的矩阵向量乘法、及 N 次高斯抽样算法，L2RS 需要执行 N 次哈希运算、3N+2 次矩阵向量乘法、及 N 次高斯抽样算法；显然，在该阶段本方案 LSLRS 效率最优。在签名验证阶段，本方案 LSLRS 需要执行一次 $\mathrm{TAcc}_{\boldsymbol{A}}()$算法、一次哈希运算、及两次矩阵乘法运算，该阶段的总时间开销为 $T_{\mathrm{H}} + (N+1)T_{\mathrm{MUL}}$；L2RS 需要执行 N 次哈希运算和 4N+1 次的矩阵向量乘法，汤永利等方案[10]需要执行 2N 次哈希运算和 2N 次的矩阵向量乘法；在该阶段本方案[10]效率最优。这里用 T(L2RS)表示 L2RS 的时间复杂度，用 T(TANG)表示汤永利等方案[10]的时间复杂度，用 T(LSLRS)表示本方案的时间复杂度，则

$$\begin{aligned}
T(\mathrm{L2RS}) &= N\cdot T_{\mathrm{MUL}} + N\cdot T_{\mathrm{LHL}} + N\cdot T_{\mathrm{H}} + \\
&(3N+2)T_{\mathrm{MUL}} + N\cdot T_{\mathrm{SD}} + N\cdot T_{\mathrm{H}} + (4N+1)T_{\mathrm{MUL}} = \\
&(8N+3)T_{\mathrm{MUL}} + N\cdot T_{\mathrm{SD}} + 2N\cdot T_{\mathrm{H}} + N\cdot T_{\mathrm{LHL}}
\end{aligned}$$

$$\begin{aligned}
T(\mathrm{TANG}) &= T_{\mathrm{TG}} + N\cdot T_{\mathrm{H}} + N\cdot T_{\mathrm{SP}} + (N+1)T_{\mathrm{H}} + \\
&(2N+1)T_{\mathrm{MUL}} + N\cdot T_{\mathrm{SD}} + 2N\cdot T_{\mathrm{H}} + 2N\cdot T_{\mathrm{MUL}} = \\
&(4N+1)T_{\mathrm{MUL}} + N\cdot T_{\mathrm{SD}} + (4N+1)T_{\mathrm{H}} + N\cdot T_{\mathrm{SP}} + T_{\mathrm{TG}}
\end{aligned}$$

$$\begin{aligned}
T(\mathrm{LSLRS}) &= N\cdot T_{\mathrm{bin}} + N\cdot T_{\mathrm{MUL}} + 3T_{\mathrm{H}} + T_{\mathrm{TAcc}} + \\
&T_{\mathrm{TWitness}} + T_{\mathrm{SD}} + T_{\mathrm{MUL}} + T_{\mathrm{bin}} + T_{\mathrm{TAcc}} + T_{\mathrm{H}} + 2T_{\mathrm{MUL}} = \\
&(N+3)T_{\mathrm{MUL}} + 2T_{\mathrm{TAcc}} + T_{\mathrm{SD}} + 4T_{\mathrm{H}} + (N+1)T_{\mathrm{bin}} + T_{\mathrm{TWitness}} = \\
&(N+3)T_{\mathrm{MUL}} + 2(N-1)T_{\mathrm{MUL}} + T_{\mathrm{SD}} + 4T_{\mathrm{H}} + (N+1)T_{\mathrm{bin}} + T_{\mathrm{TWitness}} = \\
&(3N+1)T_{\mathrm{MUL}} + (N+1)T_{\mathrm{bin}} + T_{\mathrm{TWitness}} + T_{\mathrm{SD}} + 4T_{\mathrm{H}}
\end{aligned}$$

显然 T(LSLRS)最小，本方案的效率最高。

表 1　时间开销对比

Tab. 1　Comparison of time cost

方案	系统创建	密钥生成	签名	验证
L2RS[11]	/	$N\cdot T_{\mathrm{MUL}}+$ $N\cdot T_{\mathrm{LHL}}$	$N\cdot T_{\mathrm{H}}+(3N+2)T_{\mathrm{MUL}}+N\cdot T_{\mathrm{SD}}$	$N\cdot T_{\mathrm{H}}+$ $(4N+1)T_{\mathrm{MUL}}$
文献[10]	T_{TG}	$N\cdot T_{\mathrm{H}}+N\cdot T_{\mathrm{SP}}$	$(N+1)T_{\mathrm{H}}+(2N+1)T_{\mathrm{MUL}}+N\cdot T_{\mathrm{SD}}$	$2N\cdot T_{\mathrm{H}}+2N\cdot T_{\mathrm{MUL}}$
LSLRS	/	$N\cdot T_{\mathrm{bin}}+$ $N\cdot T_{\mathrm{MUL}}$	$3T_{\mathrm{H}}+T_{\mathrm{TAcc}}+T_{\mathrm{TWitness}}+T_{\mathrm{SD}}+$ $T_{\mathrm{MUL}}+T_{\mathrm{bin}}$	$T_{\mathrm{TAcc}}+T_{\mathrm{H}}+2T_{\mathrm{MUL}}$

chinaXiv:202205.00088v1

ChinaXiv合作期刊

chinaXiv:202205.00088v1

三种方案的存储开销对比如表 2 所示，仍然统一使用 N 表示环成员个数，主要从单个用户的公钥长度、私钥长度、及签名长度分别进行对比。log 的底数为 2，$\log q>1$。在单个用户公钥长度方面，本方案 LSLRS 的公钥 $\boldsymbol{d}_i\in\{0,1\}^{nk}$，为 nk (即 $n\lceil\log q\rceil$)维的列向量，每个向量元素为 0 或 1，故单个公钥占 $n\lceil\log q\rceil$ 位；汤永利等的方案[10]公钥属于 $\mathbb{Z}_q^n$，为 n 维列向量，故长度为 $nlogq$；L2RS[11]的公钥属于卷积多项式环 $\mathcal{R}_{2q}^{1\times m}$，通常将其表示为矩阵形式(即系数矩阵)，(其系数矩阵)属于 $\mathbb{Z}_{2q}^{n\times m}$，故公钥长度为 $nm+nm\log q$；因此本方案的公钥长度与文献[10]的几乎一样，较 L2RS 有明显的减小。在单个用户私钥长度方面，本方案 LSLRS 的公钥 $\boldsymbol{x}_i\in\{0,1\}^m$，为 m 维的列向量，每个向量元素为 0 或 1，故单个公钥占 m 位；汤永利等的方案[10]私钥属于 $\mathbb{Z}_q^m$，为 m 维列向量，故长度为 $mlogq$；L2RS[11]的私钥属于卷积多项式环 $\mathcal{R}_{2q}^{m\times 1}$，通常将其表示为矩阵形式(即系数矩阵)，(其系数矩阵)属于 $\mathbb{Z}_{2q}^{m\times n}$，故私钥长度为 $nm+nm\log q$；因此，本方案的私钥长度较 L2RS 和文献[10]有明显的减小。在单个签名长度方面，本方案 LSLRS 生成的签名 $(\boldsymbol{u},I,W,\boldsymbol{c},z,\boldsymbol{k})\in\{0,1\}^{nk}\times\mathbb{Z}_q\times\mathbb{Z}_q\times\{0,1\}^{nk}\times\mathbb{Z}_q\times\mathbb{Z}_q^m$，文献[10]生成的签名 $(C_1,\boldsymbol{t}_1,\cdots,\boldsymbol{t}_N,I,\boldsymbol{b})\in\mathbb{Z}_q\times(\mathbb{Z}_q^{m+1})^N\times\mathbb{Z}_q\times\mathbb{Z}_q^n$，L2RS[11]的签名 $(\boldsymbol{c}_1,\boldsymbol{t}_1,\cdots,\boldsymbol{t}_N,\boldsymbol{H})\in\mathcal{R}_{2q}\times(\mathbb{Z}_{2q}^m)^N\times\mathcal{R}_{2q}^{1\times m}$，对比表明本方案的签名长度较 L2RS 和文献[10]有明显的减小，而且随着环成员数量 N 的增大，L2RS 和文献[10]的签名长度会随之增大，而本方案的签名长度固定不变。综上可知，本方案 LSLRS 的整体存储开销明显小于 L2RS 和文献[10]的。

表 2　存储开销对比

Tab. 2　Comparison of storage overhead

方案	公钥长度	私钥长度	签名长度
L2RS[11]	$nm+nmlogq$	$nm+nmlogq$	$(n+mN+nm)(1+logq)$
文献[10]	$nlogq$	$mlogq$	$[(m+1)N+n+2]logq$
LSLRS	$n\lceil\log q\rceil$	m	$m+(m+3)logq$

5.2　实验评估

本文的实验在配置为 Win10 系统、英特尔酷睿 i7-10750H@2.60GHz 处理器、512GB 固态硬盘、8GB 内存的计算机上运行，将参数设置为 n=8，m=512，$q=2^{32}$。

表 3 为三个方案(L2RS[11]、文献[10]、本方案 LSLRS)的时间开销统计，环成员个数为 16；图 1 为依据表 3 中的数据画出的时间开销对比图。从表 3 和图 1 中可以看出，本方案 LSLRS 在系统创建、签名、验证阶段的时间开销最小，方案的总时间开销也是最小的，效率最高，具体原因已在上节进行了分析，此处不再赘述。

表 3　时间开销统计(单位：ms，N=16)

Tab. 3　Statistics of time cost

方案	系统创建	密钥生成	签名	验证	总时间
L2RS[11]	0.012	12.096	29.364	30.426	71.898
文献[10]	0.348	5.952	21.364	14.976	42.64
LSLRS	0.009	7.176	12.144	6.988	26.317

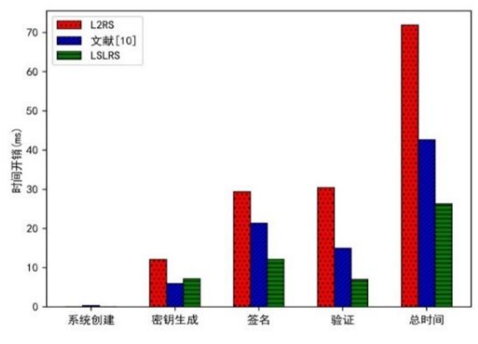


图 1　时间开销对比(N=16)

Fig. 1　Comparison of time cost (N=16)

表 4 为三个方案(L2RS[11]、文献[10]、本方案 LSLRS)的存储开销统计，图 2 为依据表 4 中的单个公私钥长度数据画出的密钥长度对比图，图 3 为依据表 4 中的签名长度数据画出的签名长度对比图。从表 4 和图 2 可以看出，本方案 LSLRS 的单个公钥长度较小，单个私钥长度最小；从表 4 和图 3 可以看出，本方案 LSLRS 的签名长度最小，随着环成员个数的增大，L2RS[11]与文献[10]的签名长度均在增大，而本方案的签名长度保持不变，具体原因见上节的分析。

表 4　存储开销统计(单位：KB)

Tab. 4　Statistics of storage overhead

方案	单个公钥长度	单个私钥长度	签名长度			
			N=4	N=16	N=64	N=256
L2RS[11]	16.5	16.5	24.782	49.532	148.532	544.532
文献[10]	0.031	2	8.055	32.102	128.289	516.039
LSLRS	0.031	0.063	2.074	2.074	2.074	2.074

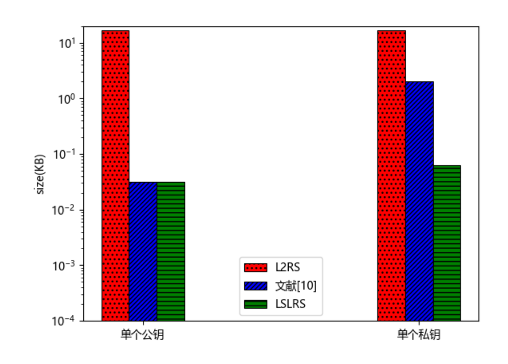


图 2　密钥长度对比

Fig. 2　Comparison of key size

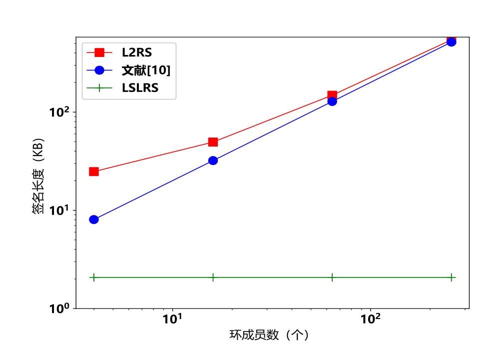


图 3　签名长度对比

Fig. 3　Comparison of signature size

6　结束语

可链接环签名能有效解决区块链电子货币系统的双花攻击与区块链电子选举系统的重复投票问题，但已有基于格的可链接环签名长度随环成员的增多而增大，本文提出了基于格的简短可链接环签名。随着环成员的增多，本文 LSLRS 的签名长度保持不变，同时节省了时间和存储开销，因此本文方案具有更强的实用性。基于 SIVP 问题证明了签名的不可伪造性，另外又证明了签名的匿名性和可链接性。下一步工作致力于提出具体的基于格的区块链安全应用方案，并进一步提高方案的效率，确保区块链技术能更好地为社会大众服务。

参考文献：

[1] Yang Di, Long Chengnian, Xu Han, *et al.* A review on scalability of blockchain [C]// Proc of the 2nd International Conference on Blockchain Technology. New York: ACM Press, 2020: 1-6.

ChinaXiv合作期刊

chinaXiv:202205.00088v1

[2] 蔡晓晴，邓尧，张亮，等. 区块链原理及其核心技术 [J] 计算机学报, 2021, 44 (01): 84-131. (Cai Xiaoqing, Deng Yao, Zhang Liang, *et al.* The principle and core technology of blockchain [J]. Chinese Journal of Computers, 2021, 44 (01): 84-131.)

[3] Rivest R L, Shamir A, Tauman Y. How to leak a secret [C]// Proc of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Berlin: Springer, 2001: 552-565.

[4] 范青，何德彪，罗敏，等. 基于SM2数字签名算法的环签名方案 [J]. 密码学报, 2021, 8 (4): 710-723. (Fan Qing, He Debiao, Luo Min, *et al.* Ring signature schemes based on SM2 digital signature algorithm [J]. Journal of Cryptologic Research, 2021, 8 (4): 710－723.)

[5] Liu J K, Wei V K, Wong D S. Linkable spontaneous anonymous group signature for ad hoc groups [C]// Proc of the 9th Australasian Conference on Information Security and Privacy. Berlin: Springer, 2004: 325-335.

[6] Lyu Jiazhuo, Jiang Z L, Wang Xuan, *et al.* A secure decentralized trustless e-voting system based on smart contract [C]// Proc of the 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Los Alamitos: IEEE Computer Soc. Press, 2019: 570-577.

[7] Tsang P P, Wei V K. Short linkable ring signatures for e-voting, e-cash and attestation [C]// Proc of the 1st Information Security Practice and Experience Conference. Berlin: Springer, 2005: 48-60.

[8] Au M H, Chow S S M, Susilo W, *et al.* Short linkable ring signatures revisited [C]// Proc of the 3rd European Public Key Infrastructure Workshop. Berlin: Springer, 2006: 101-115.

[9] Yu Bin, Liu J K, Sakzad A, *et al.* Platform-independent secure blockchain-based voting system [C]// Proc of the 21st International Information Security Conference. Berlin: Springer, 2018: 369-386.

[10] 汤永利，夏菲菲，叶青，等. 格上基于身份的可链接环签名 [J]. 密码学报, 2021, 8 (2): 232-247. (Tang Yongli, Xia Feifei, Ye Qing, *et al.* Identity-based linkable ring signature on lattice [J]. Journal of Cryptologic Research, 2021, 8 (2): 232-247.)

[11] Torres W A, Kuchta V, Steinfeld R, *et al.* Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1. 0) [C]// Proc of the 23rd Australasian Conference on Information Security and Privacy. Berlin: Springer, 2018: 558-576.

[12] Torres W A, Kuchta V, Steinfeld R, *et al.* Lattice RingCT v2. 0 with multiple input and multiple output wallets [C]// Proc of the 24th Australasian Conference on Information Security and Privacy. Berlin: Springer, 2019: 156-175.

[13] Baum C, Huang Lin, Oechsner S. Towards practical lattice-based one-time linkable ring signature [C]// Information and Communications Security. Proc of the 20th International Conference. [S. I.] : LNCS, 2018: 303-322.

[14] Liu Zhen, Nguyen K, Yang Guomin, *et al.* A lattice-based linkable ring signature supporting stealth addresses [C]// Proc of the 24th European Symposium on Research in Computer Security. [S. I.] : LNCS, 2019: 726-746.

[15] Saberhagen N V. CroptoNote v2. 0 [EB/OL]. (2013-10-17) [2022-02-08]. https://static. coinpaprika. com/storage/cdn/whitepapers/1611. pdf.

[16] 叶青，王文博，李莹莹，等. 利用环上容错学习问题构造可链接环签名方案 [J]. 计算机科学与探索, 2020, 14 (7): 1164-1172. (Ye Qing, Wang Wenbo, Li Yingying, *et al.* Using ring learning with errors problem to construct linkable ring signature scheme [J]. Journal of Frontiers of Computer Science and Technology, 2020, 14 (7): 1164-1172.)

[17] 庄立爽，陈杰，王启宇. 电子投票协议下的基于格的可链接门限环签名 [J]. 密码学报, 2021, 8 (3): 402－416. (Zhuang Lishuang, Chen Jie, Wang Qiyu. Lattice-based linkable threshold ring signature in e-voting [J]. Journal of Cryptologic Research, 2021, 8 (3): 402－416.)

[18] 严蔚敏，李冬梅，吴伟民. 数据结构: C 语言版 [M]. 2 版. 北京：人民邮电出版社, 2015: 55. (Yan Weimin, Li Dongmei, Wu Weimin. Data Structure [M]. 2nd ed. Beijing: Posts & Telecom Press, 2015: 55.)

[19] Camenisch J, Stadler M. Efficient group signature schemes for large groups (extended abstract) [C]// Proc of the 17th Annual International Cryptology Conference. Berlin: Springer, 1997: 410-424.

[20] Libert B, Ling S, Nguyen K, *et al.* Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors [C]// Proc of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2016, 9666: 1-31.

[21] Lyubashevsky V. Lattice signatures without trapdoors [C]// Proc of the 31st Annual IACR Eurocrypt International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 738–755.

[22] 杨波. 现代密码学 [M]. 4 版. 北京：清华大学出版社, 2017: 273-274. (Yang Bo. Modern cryptography [M]. 4th ed. Beijing: Tsinghua University Press, 2017: 273-274.)

[23] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions [C]// Proc of the 14th Annual ACM International Symposium on Theory of Computing. New York: ACM Press, 2008: 197–206.